**Кібербезпека в умовах війни**

Анотація. Основна увага цього дослідження зосереджена на забезпеченні кібербезпеки соціально-економічної системи під час воєнного стану. Враховуючи зростаюче значення кібербезпеки в сучасному світі, особливо в умовах ескалації кіберзагроз у контексті глобальних конфліктів, ваші дослідження мають важливе значення для зміцнення економічної безпеки нації. Сфера кібербезпеки дуже динамічна, загрози постійно розвиваються. Під час війни співпраця з іншими державами та міжнародними організаціями може мати вирішальне значення для забезпечення кібербезпеки.

**Основною метою** дослідження є визначення методів і стратегій забезпечення кібербезпеки соціально-економічної системи в умовах воєнного стану.

**Предметом дослідження** є сама система кібербезпеки.

Ключові слова: КІБЕРБЕЗПЕКА, КІБЕЗАГРОЗИ, ВІЙНА, КІБЕРЗАХИСТ

Цифровізація, безсумнівно, проникла в усі аспекти людської діяльності. У сучасну цифрову епоху атаки на цифрову інфраструктуру стали невід’ємним аспектом війни через серйозні соціально-економічні наслідки, перешкоди ефективним заходам протидії та виснаження ресурсів. Крім того, створення цифрових загроз часто потребує відносно скромних інвестицій і створює мінімальний ризик для зловмисників, але потенційна можливість завдати значної шкоди є великою. Тому оцінка ризиків і відчутних загроз економічній безпеці в цифровій сфері, а також належна підготовленість і своєчасне реагування набувають першочергового значення. Це особливо актуально на тлі ескалації глобальної напруженості та конфліктів, таких як російське вторгнення в Україну.

Основною метою кібервійни є досягнення конкретних цілей в економічній, політичній, військовій та інших областях. Крім того, існує вторинна мета, яка передбачає цілеспрямований вплив на суспільство та владу через заздалегідь продумані інформаційні кампанії. Отже, кібервійна має психологічний вимір і діє як форма інформаційної війни, що ведеться в кіберпросторі. Враховуючи повсюдне поширення комп’ютерних технологій та Інтернету в повсякденному житті людей, підприємств і державних установ у всьому світі, маніпулювання даними, що надходять від цих організацій, становить значну загрозу національній безпеці. Отже, кібербезпека виступає як невід’ємний елемент забезпечення національної безпеки в умовах цього складного протистояння [1].

Метою цього дослідження є визначення стратегій забезпечення кіберстійкості соціально-економічної системи в умовах воєнного стану. Предметом дослідження є система кібербезпеки.

Важливо підкреслити складний і багатогранний характер цифрової ери, де технологічний прогрес створює як можливості, так і ризики. Вирішення цих проблем вимагає цілісного підходу, який охоплює міжнародну співпрацю, протоколи кібербезпеки та відповідальне використання цифрових технологій. Кібербезпека для бізнесу в Україні має першочергове значення в сучасному цифровому ландшафті. Як і в багатьох інших країнах, український бізнес стикається з численними кіберзагрозами, які можуть призвести до фінансових втрат, шкоди репутації та збоїв у роботі. Ось ключові аспекти кібербезпеки для бізнесу в Україні:

1. Системи захисту: Важливо впроваджувати надійні системи захисту кібербезпеки. Це включає використання найновішого антивірусного програмного забезпечення, брандмауерів, систем виявлення та запобігання вторгненням, а також інструментів шифрування для захисту конфіденційних даних.

2. Регулярні оновлення програмного забезпечення: Важливо підтримувати все програмне забезпечення та операційні системи на комп’ютерах і серверах компанії в актуальному стані. Кіберзлочинці часто використовують уразливості в застарілому програмному забезпеченні, які можна виправити за допомогою оновлень.

3. Навчання співробітників: Регулярне навчання та навчання співробітників передовим практикам кібербезпеки є життєво важливим. Співробітники повинні знати про типові загрози, такі як фішингові атаки, і знати, як на них реагувати.

4. Захист від внутрішніх загроз: Окрім зовнішніх загроз, компанії повинні зосередитися на заходах внутрішньої безпеки. Це може включати обмеження доступу до конфіденційної інформації та мережевих ресурсів лише тим, хто цього потребує.

5. Резервне копіювання даних: Регулярне резервне копіювання важливих даних є фундаментальною частиною кібербезпеки. Ця практика гарантує можливість відновлення даних у разі кібератаки, витоку даних або інших несподіваних інцидентів.

6. План реагування на інциденти: Важливо мати чітко визначений план реагування на інциденти. У цьому плані описано кроки, яких необхідно вжити у разі порушення кібербезпеки, і він допомагає зменшити потенційну шкоду.

7. Відповідність нормам: Україна має спеціальні норми, пов’язані з кібербезпекою. Підприємства повинні забезпечити дотримання цих правил, щоб уникнути юридичних проблем і штрафів.

8. Кіберстрахування: Деякі компанії вирішують придбати кіберстрахування, щоб захиститися від фінансових втрат у результаті кібератак.

9. Регулярні аудити безпеки: Проведення регулярних аудитів і оцінок безпеки може допомогти виявити вразливі та слабкі місця в інфраструктурі кібербезпеки.

10. Співпраця та обмін інформацією: Обмін інформацією та співпраця з іншими підприємствами, галузевими організаціями та правоохоронними органами може допомогти підвищити обізнаність про нові загрози та поділитися передовим досвідом.

11. Моніторинг і виявлення: Розгортання систем моніторингу для виявлення потенційних інцидентів безпеки та реагування на них має вирішальне значення для випередження кіберзагроз.

12. Міжнародне співробітництво: Кіберзагрози не обмежені кордонами. Міжнародна співпраця та обмін інформацією можуть мати неоціненне значення для боротьби з кібератаками та їх запобігання.

Підсумовуючи, підприємства в Україні повинні активно підходити до кібербезпеки, поєднуючи технології, освіту та найкращі практики, щоб захистити свою діяльність, конфіденційні дані та репутацію у все більш цифровому світі.Отже, забезпечення кібербезпеки в Україні потребує комплексного підходу, що включає технічні, освітні, організаційні та правові заходи. Регулярне оновлення та вдосконалення протоколів кібербезпеки є обов’язковим для ефективної боротьби з постійно зростаючими кіберзагрозами. Інформація є одним із найвпливовіших інструментів у політиці, особливо на міжнародній арені. Маніпулювання інформацією може посилити напругу, особливо під час конфлікту, і сформувати сприйняття фактів відповідно до інтересів тих, хто прагне впливати. Важливо визнати, що еволюція цифрових медіа та ліквідація інформаційних кордонів зробили нації більш відкритими та сприйнятливими до втручання інших держав у їхні політичні та інформаційні сфери. Інформаційний ландшафт глибоко впливає на економічні, політичні та культурні процеси, а також на траєкторію військових стратегій і технологій. З прискоренням переходу до цифрового управління загроза кібербезпеці зростає, особливо для таких країн, як Україна, які постійно були стратегічними цілями зовнішньої політики Росії. Отже, забезпечення кібербезпеки під час конфлікту набуває першорядної важливості, оскільки практично кожен компонент технологічної інфраструктури тепер інтегрує різні програмні системи, багато з яких підключені до Інтернету, що створює значні ризики.

У цьому контексті кібератаки можуть слугувати додатковим інструментом у сфері інформаційної війни, призначеним для зламу та викриття секретних даних або поширення сфабрикованої інформації, яка часто маскується під надійні джерела. Усі ці міркування вимагають прийняття нового підходу до кібербезпеки, особливо щодо критичної інфраструктури та систем життєзабезпечення. Загрози в кіберпросторі створюють найстрашніші виклики національній безпеці України, виходячи за межі ключових сфер, таких як економіка, політика, суспільство та військо. На жаль, кібербезпека залишається менш зрозумілою та недооціненою загрозою. Необхідно усвідомити, що зараз кіберпростір є основним театром бойових дій. Прагнення до кібердомінування та спроможності протистояти кібератакам віщує нову еру у військових відносинах, змінюючи природу та структуру збройних сил.

Крім того, важливо підкреслити, що досягнення кібербезпеки не може обмежуватися лише державним рівнем. Це вимагає інтеграції зусиль приватного сектору, бізнесу, а також міжнародної координації та співпраці в безпрецедентних масштабах.

**Список використаних джерел**

1. Іжа, М., Пахомова, Т., Липач, О., Якубовський, О., & Ахламов, . Моделювання забезпечення кібербезпеки соціально-економічної системи в умовах воєнного стану. Financial and Credit Activity Problems of Theory and Practice, 3(50), 2023. С. 224–233.
2. Kryshtanovych, M., Lyubomudrova, N., Bondar, H., Motornyy, V., & Kuchmenko, V.. An intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. Ingénierie des Systèmes d’Information, Vol. 28, No. 1, 2023. P. 41-47.
3. Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3), 2022, P. 299-310.
4. Rodrigues, A.R.D., Ferreira, F.A., Teixeira, F.J., & Zopounidis, C.. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. Research in International Business and Finance, 60, 2022. P. 101- 116.
5. Shakhatreh, H.. Payment of canal dues by carriers carrying out international overseas transportation – A case of legal discrimination. Studia Iuridica Lublinensia, 32(1). 2023 P. 251-273